

OS X: About FileVault 2

With FileVault 2 you can encrypt the contents of your entire drive to help keep your data secure.

<http://support.apple.com/kb/ht4790>

FileVault 2 uses full disk, XTS-AES 128 encryption to help keep your data secure. Using FileVault 2, you can encrypt the contents of your entire drive.



Why should you encrypt your data?

Data encryption is a method of disguising your data. Therefore, even if someone did get ahold of your flash drive that had video data on it, they wouldn't be able to see it without having a password to decrypt it. One way to encrypt your data is with *TrueCrypt*. *TrueCrypt* is a "free open-source disk encryption software". The following steps will walk you through how to encrypt your flash drive using *TrueCrypt*.

What You'll Need:

- Computer with Internet Access
- Clean Flash Drive (8-16GB+)

BEFORE YOU START: Make sure that no data is on the flash drive that you plan on encrypting since it could potentially get erased in the process of formatting or encrypting!

FileVault 2 requirements

FileVault 2 requires OS X Lion or later, and [OS X Recovery](http://support.apple.com/kb/HT4718) installed on your startup drive.
<http://support.apple.com/kb/HT4718>

Turning on FileVault 2

FileVault 2 is available from the Security & Privacy pane of System Preferences. Click the FileVault tab in the Security & Privacy pane to enable or disable FileVault.

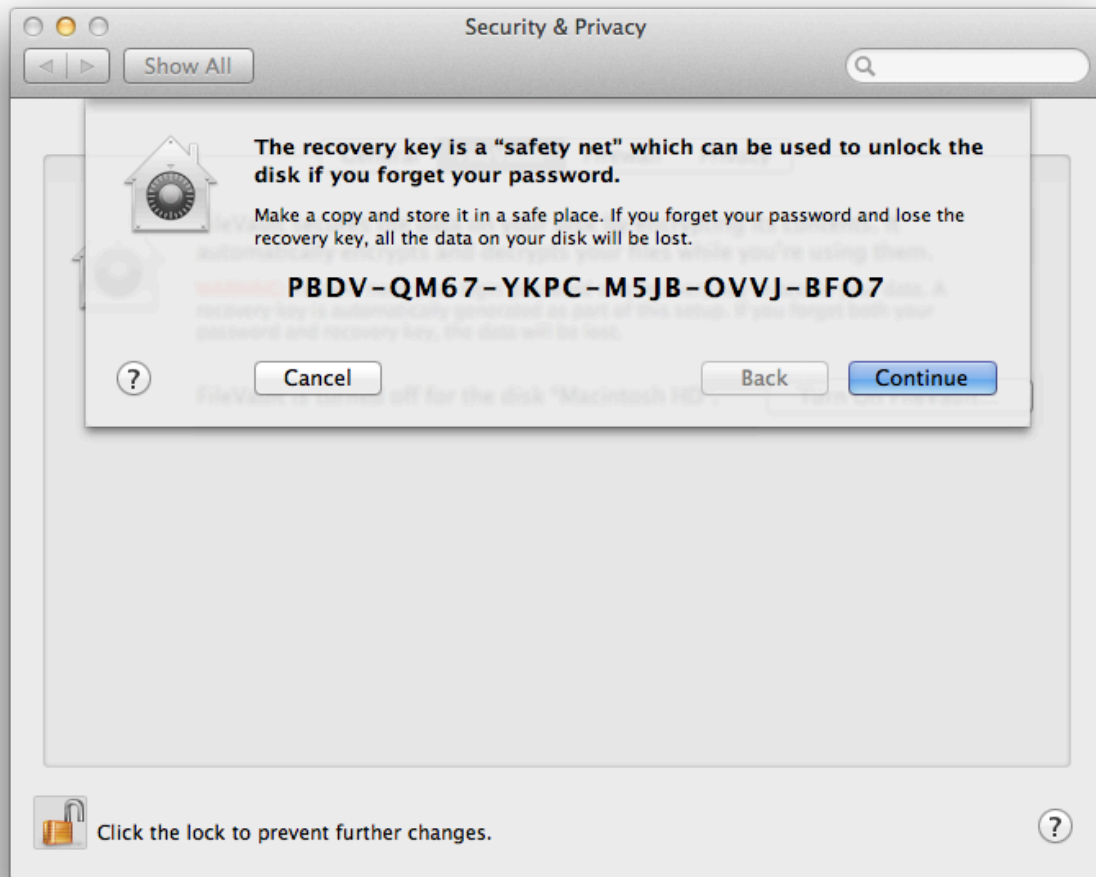
If you migrated a home directory that was encrypted by an earlier version of FileVault (Legacy Filevault), you need to turn this off first. See the "Migrating a FileVault-protected Home from an earlier version of Mac OS X" section below for more information.

When you select "Turn On FileVault", you're asked to identify the user accounts that are allowed to unlock the encrypted drive if there is more than one account present. You'll need to enter the password (or have users enter their passwords) for each account you want to have the ability to unlock FileVault 2.



Users not enabled for FileVault unlock are only able to log into the computer after an unlock-enabled user has started or unlocked the drive. Once unlocked, the drive remains unlocked and available to all users, until the computer is restarted.

After selecting which users can unlock the disk, you're shown your recovery key.



This key is a backup unlock method provided to you in case the unlock-enabled user password is forgotten. You can highlight and copy this key to print it out, email it, or otherwise copy it. Remember that maintaining a copy of this key on your computer does not help you if you forget your login password. Your drive will remain encrypted and inaccessible along with the rest of your data. Make an external copy of this key, or write it down and store it in a secure but retrievable location.

You can also store your recovery key with Apple. See the "Storing your recovery key with Apple" section below for more information.

After you've completed the process of turning on FileVault, you're prompted to restart your Mac. After restarting, a login screen appears. Select your account name and enter your password to continue. This unlocks the disk. Next, an Apple logo with a spinning gear underneath it appears, and the computer continues starting up.

The user account that unlocked the drive is automatically logged in after start up completes. The first time you log in after turning on FileVault, the initial encryption of your entire hard disk begins. It should complete within a few hours. This happens in the background, and doesn't interrupt normal usage of your computer. In addition to using your computer while encryption is happening, you can sleep, log out and even turn off your computer during this time. Encryption continues when your computer is powered on again.

Choose a topic below to learn more about additional features of FileVault 2.

Storing your recovery key with Apple

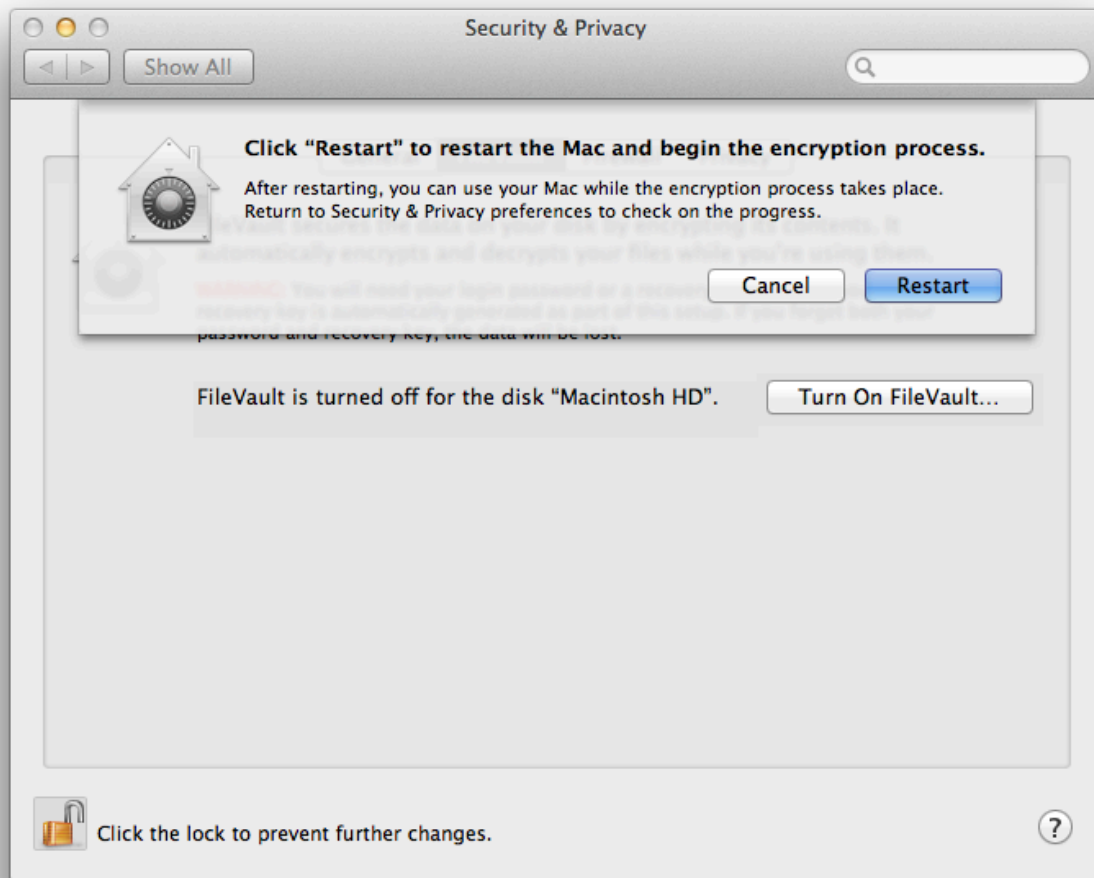
After you are shown your recovery key, you are also given the opportunity to store your recovery key with Apple.



If you choose to store your key with Apple, you're presented with three "Choose a question" menus with three corresponding answer fields.



The key you store with Apple is encrypted, along with the answers you provide. Carefully choose questions and answers that you can easily remember exactly as you typed them. This is important if you later need to retrieve your recovery key from Apple. Click Continue to send your key to Apple. Your computer restarts after this step, to begin FileVault disk encryption.



Retrieving your recovery key from Apple

If you forget your login password for a FileVault-encrypted drive, but you stored your recovery key with Apple, you can contact AppleCare and request retrieval of your recovery key.

Typing in the wrong login password three times prompts you if you have the ability to retrieve your key from Apple. Click the triangle-button next to the prompt that appears to reveal a Recovery Key text field (which replaces the password text field) and AppleCare contact information, along with your computer's Serial Number and a Record Number. You need to provide these pieces of information in order for AppleCare to retrieve your recovery key.

Upon successful retrieval and entry of your recovery key, you are prompted to change your login password. After changing your login password, it's also recommended that you change your FileVault recovery key and upload the new one to Apple.

Changing your recovery key

In the Security & Privacy system preference, under the FileVault tab, click "Turn Off FileVault" to disable FileVault. After FileVault is off, FileVault will begin to decrypt your drive. Once decryption is complete, you can click the "Turn On FileVault" button. Doing this allows you to enable unlock-capable users. You're also provided with a new recovery key and have the option of sending this new key to Apple. The old key sent to Apple will not be able to unlock your newly-encrypted disk. If you need to retrieve your recovery key from Apple, only the new one will be retrieved based on the Serial Number and Record Number displayed in the login window.

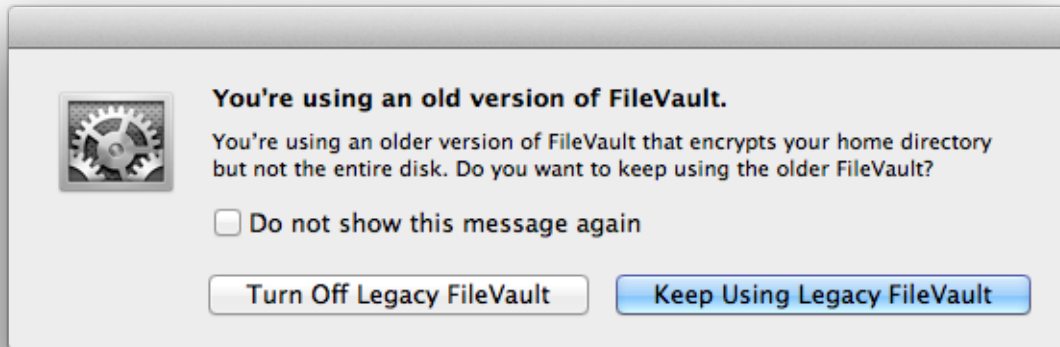
Letting other users unlock the drive

If you want to make the Mac available to a user that doesn't currently have unlock capabilities, log in as a user that can unlock the disk. When you see your own desktop, choose "Log Out (*user name*)" from the Apple (☐) menu. Also, you unlock the disk, then switch to another user from Fast User Switch menu in the menu bar.

If you want to grant existing users the ability to unlock the drive on their own, open the Security & Privacy pane of System Preferences. Select the FileVault tab and click the lock icon in the lower left corner of the window. Enter your admin privileges when prompted. Click the "Enable Users..." button to add existing users to the list of accounts that can unlock the disk.

Migrating a Legacy FileVault home folder from an earlier version of OS X

If you're using FileVault in Mac OS X v10.6 Snow Leopard, you can upgrade to a later version of OS X and continue to use your FileVault-encrypted home directory. In OS X Lion and later this version of FileVault encryption is known as "Legacy FileVault". With a Legacy FileVault encrypted home directory, opening the Security & Privacy preference pane alerts you that "You're using an old version of FileVault."



You can continue to use OS X with Legacy FileVault, but you can't enable Legacy FileVault for other user accounts in OS X Lion or later. If you turn off Legacy FileVault, the Legacy FileVault tab goes away. Use the FileVault tab that remains to enable the newer FileVault 2 encryption method.

Additional support

If you have need of further help then please contact the UWO Help Desk at 920-424-3020 or visit them at Dempsey Room 207.